

# Modelling and Analysis of Network Security - a Probabilistic Value-passing CCS Approach

Qian Zhang  
State Key Laboratory of  
Computer Science, Institute of  
Software Chinese Academy of  
Sciences  
Beijing, China  
zhangq@ios.ac.cn

Ying Jiang  
State Key Laboratory of  
Computer Science, Institute of  
Software Chinese Academy of  
Sciences  
Beijing, China  
jy@ios.ac.cn

Liping Ding  
National Engineering  
Research Center for  
Fundamental  
Software, Institute of Software  
Chinese Academy of Sciences  
Beijing, China  
liping@nfs.iscas.ac.cn

## ABSTRACT

In this work, we propose a probabilistic value-passing CCS (Calculus of Communicating System) approach to model and analyze a typical network security scenario with one attacker and one defender. By minimizing this model with respect to probabilistic bisimulation and abstracting it through graph-theoretic methods, two algorithms based on backward induction are designed to compute Nash Equilibrium strategy and Social Optimal strategy respectively. For each algorithm, the correctness is proved and an implementation is realized. Finally, this approach is illustrated by a detailed case study.

## Categories and Subject Descriptors

C.2.0 [Computer-Communication Networks]: General—*Security and protection*

## General Terms

Security

## Keywords

Network security; Nash equilibrium strategy; Social optimal strategy; Reactive model; Probabilistic value passing CCS

## 1. INTRODUCTION

Modeling and analysis of network security has been a hot research spot in the network security domain. It has been studied from different perspectives. Among them are two main approaches, one based on game-theoretic methods [15], and one based on (probabilistic) process algebra [13, 22, 4]. In the later 1990's, game theoretic methods were introduced for modeling and analyzing network security [21]. These methods consist in applying different kinds of games to different network scenarios with one attacker and one defender [17]. Roughly speaking, *static game* is a one-shot game in

which players choose action simultaneously. It is often used to model the scenarios in which the attacker and defender have no idea on the action chosen by the adversary (for instance the scenario of information warfare), and to compute the best strategy for players in a quantitative way [9]. *Stochastic game* is often used to model the scenarios which involve probabilistic transitions through states of network systems according to the actions chosen by the attacker and the defender [10, 12]. *Markov game* is an extension of game theory to MDP-like environments [23]. It is often used to model the scenarios in which the future offensive-defensive behaviors will impact on the present action choice of attacker and defender [24]. In *Bayesian game*, the characteristics about other players is incomplete and players use Bayesian analysis in predicting the outcome [7]. A dynamic Bayesian game with two players, called *Signaling game*, is often used to model intrusion detection in mobile ad-hoc networks and to analyze Nash equilibrium in a qualitative way [16]. On the other hand, as far as we know, (probabilistic) process algebra approach focus on verifying network security protocols. For example, in the earlier 1980's, a simple version of the alternating bit protocol in  $ACP_\tau$  (Algebra of Communicating Processes with silent actions) was verified [2]. For describing and analyzing cryptographic protocols, the spi calculus, an extension of the  $\pi$  calculus, was designed [1]. Recently, a generalization of the bisimilarity pseudo-metric based on the Kantorovich lifting is proposed, this metric allows to deal with a wider class of properties such as those used in security and privacy [3].

In this paper, we propose a probabilistic value-passing CCS (PVCCS) approach for modeling and analyzing a typical network security scenario with one attacker and one defender. A network system is supposed to be composed of three participants: one attacker, one defender and the network environment which is the hardware and software services of the network under consideration. We consider all possible behaviors of the participants at each state of the system as processes and assign each state with a process describing all possible interactions currently performed among the participants. In this way we establish a network state transition model, often called reactive model in the literature [22], based on PVCCS. By minimizing this model with respect to probabilistic bisimulation and abstracting it via graph-theoretic methods, two algorithms based on backward

induction are designed to compute Nash Equilibrium Strategy (NES) [11, 8, 20] and Social Optimal Strategy (SOS) [14, 6] respectively. The former represents a stable strategy of which neither the attacker nor the defender is willing to change the current situation, and the latter is the policy to minimize the damages caused by the attacker. For each algorithm, the correctness is proved and an implementation is realized. This approach is illustrated by a detailed case study on an example introduced in [12]. The example describes a local network connected to Internet under the assumption that the firewall is unreliable, and the operating system on the machine is insufficiently hardening, and the attacker has chance to pretend as a root user in web server, stealing or damaging data stored in private file server and private workstation. The major contributions of our work are:

- establish a reactive model based on PVCCS for a typical network security scenario which is usually modeled via perfect and complete information games.
- minimize the state space of network system via probabilistic bisimulation and abstract it via graph-theoretic methods. This allows us to reduce the search space and hence considerably optimize the complexity of the concerned algorithms.
- propose two algorithms to compute Nash Equilibrium and Social Optimal strategy respectively. The novelty consists in combing graph-theoretic methods with backward induction, which enables us on the one hand to increase reuseness and on the other hand to make the backward induction possible in the setting of some infinite paths.

Note that our method can filter out invalid Nash Equilibrium strategies from the results obtained by traditional game-theoretic methods. For instance, in the example introduced in [12], three Nash Equilibrium strategies obtained ultimately by game-theoretic approach methods, while only two of them obtained by our method: we filter out the invalid Nash Equilibrium strategy from the results in [12]. Note also our method can be applied to other network security scenarios. For example, the proposed reactive model can be extended conservatively to a generative model based on PVCCS. In this way we provide a uniform framework for modeling and analyzing network security scenarios which are usually modeled either via perfect and complete information games or via perfect and incomplete games. However, for the limited space of this paper, we will focus on the reactive setting for the conciseness and easier understanding of this work.

In the remaining sections, we shall review some notions of graph theory and establish the reactive model based on PVCCS (Section 2); present the formal definitions of NES and SOS in this model, as well as the corresponding algorithms and their correctness proofs (Section 3); then illustrate our method by a case study (Section 4); finally, discuss the conclusion (Section 5). Appendix shows proofs of theorems, tables referred to the case study and a notation index.

## 2. PRELIMINARIES AND REACTIVE MODEL BASED ON PVCCS

### 2.1 Graph theory

We firstly recall some notions of graph theory: Strongly Connected Component (SCC), Directed Acyclic Graph (DAG) and Path Contraction [5, 19, 6].

**SCC** of an arbitrary directed graph form a partition into subgraphs that are themselves strongly connected (it is possible to reach any vertex starting from any other vertex by traversing edges in the direction).

**DAG** is a directed graph with no directed cycles. There are two useful DAG related properties we used in our paper: (1) if  $H$  is a weakly connected graph,  $H'$  is obtained by viewing each SCC in  $H$  as one vertex,  $H'$  must be a DAG; (2) if  $H$  is a DAG,  $H$  has at least one vertex whose out-degree is 0.

**Path Contraction** Let  $e = xy$  be an edge of a graph  $H = (V, E)$ .  $H/e$  is a graph  $(V', E')$  with vertex set  $V' := (V \setminus \{x, y\}) \cup \{v_e\}$ , and edge set  $E' := \{vw \in E \mid \{v, w\} \cap \{x, y\} = \emptyset\} \cup \{v_e w \mid xw \in E \setminus \{e\} \text{ or } yw \in E \setminus \{e\}\}$  (Figure 1). Path contraction occurs upon the set of edges in a path that contract to form a single edge between the endpoints of the path after a series of edge contractions.

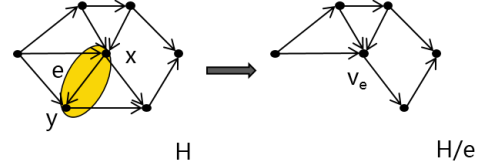


Figure 1: Edge contraction

### 2.2 PVCCS<sub>R</sub>

PVCCS<sub>R</sub> is a reactive model for Probabilistic Value-passing CCS, proposed based on the reactive model for probabilistic CCS [22].

**Syntax:** Let  $\mathcal{A}$  be a set of channel names ranged over by  $a$ , and  $\bar{\mathcal{A}}$  be the set of co-names, i.e.,  $\bar{\mathcal{A}} = \{\bar{a} \mid a \in \mathcal{A}\}$ , and  $\bar{a} = a$  by convention. **Label** =  $\mathcal{A} \cup \bar{\mathcal{A}}$ . **Var** is a set of value variables ranged over by  $x$  and **Val** is a value set ranged over by  $v$ . **e** and **b** denote value expression and boolean expression respectively. The set of actions, ranged over by  $\alpha$ , **Act** =  $\{a(x) \mid a \in \mathcal{A}\} \cup \{\bar{a}(e) \mid \bar{a} \in \bar{\mathcal{A}}\} \cup \{\tau\}$ , where  $\tau$  is the silent action.  $\mathcal{K}$  and  $\mathcal{X}$  are a set of process identifiers and a set of process variables respectively. Each process identifier  $A \in \mathcal{K}$  is assigned an arity, a non-negative integer representing the number of parameters which it takes.

**Pr** is the set of processes in PVCCS<sub>R</sub> defined inductively as follows, where  $P, P_i$  are already in **Pr**:

$$\begin{aligned} \mathbf{Pr} ::= & Nil \mid \sum_{i \in I} \sum_{j \in J} [p_{ij}] \alpha_i.P_{ij} \mid P_1 | P_2 \mid P \setminus R \\ & \mid \text{if } \mathbf{b} \text{ then } P_1 \text{ else } P_2 \mid A(x) \\ \alpha ::= & a(x) \mid \bar{a}(e) \end{aligned}$$

where  $a \in \mathbf{Label}$ ,  $R \subseteq \mathcal{A}$ .  $I, J$  are index sets, and  $\forall i \in I$ ,  $p_{ij} \in (0, 1]$ ,  $\sum_{j \in I} p_{ij} = 1$ , and  $\alpha_i \neq \alpha_j$  if  $i \neq j$ .  $\sum$  and  $\dot{\sum}$  are summation notations for processes and real numbers respectively. Furthermore, each process constant  $A(x)$  is defined recursively by associating to each identifier an equation of the form  $A(x) \stackrel{\text{def}}{=} P$ , where  $P$  contains no process variables and no free value variables except  $x$ .

$Nil$  is an empty process which does nothing;  $\sum_{i \in I} \sum_{j \in J} [p_{ij}] \alpha_i . P_{ij}$  is a summation process with probabilistic choice which means if performs action  $\alpha_i$ ,  $P_{ij}$  will be chosen to be proceed with probability  $p_{ij}$ , for example,  $[0.2] \alpha . P_1 + [0.8] \alpha . P_2 + [1] \beta . P_3$  is a process which will choose process  $P_1$  with probability 0.2 and  $P_2$  with probability 0.8 if performs action  $\alpha$ , or will choose  $P_3$  with probability 1 if performs action  $\beta$ , here  $\alpha_i$  stands for an action prefix and there are two kinds of prefixes: input prefix  $a(x)$  and output prefix  $\bar{a}(e)$ . If  $J$  is a singleton set, then we will omit the probability from the summation process, such as  $\sum_{i \in I} \sum_{j \in J} [1] \alpha_i . P_{ij}$  will be written as  $\sum_{i \in I} \alpha_i . P_i$ , and if both  $I$  and  $J$  are singleton sets, then the summation process is written as  $\alpha . P$ ;  $P_1 | P_2$  represents the combined behavior of  $P_1$  and  $P_2$  in parallel;  $P \setminus R$  is a channel restriction, whose behavior is like that of  $P$  as long as  $P$  does not perform any action with channel  $a \in R \cup \bar{R}$ ; *if  $b$  then  $P_1$  else  $P_2$*  is a conditional process which enacts  $P_1$  if  $b$  is *true*, else  $P_2$ .

**Semantics:** The operational semantics of PVCCS<sub>R</sub> is defined by the rules in Table 1, where  $P \xrightarrow{\alpha[p]} Q$  describes a transition that, by performing an action  $\alpha$ , starts from  $P$  and leads to  $Q$  with probability  $p$ . Mapping  $chan : \mathbf{Act} \rightarrow \mathcal{A}$ , i.e.,  $chan(a(x)) = chan(\bar{a}(e)) = a$ . And  $P\{e/x\}$  means substituting  $e$  for every free occurrences of  $x$  in process  $P$ . By convention, if  $P_1 \xrightarrow{\alpha[p]} P_2$  and  $P_2 \xrightarrow{\beta[q]} P_3$ , then we use  $P_1 \xrightarrow{\alpha[p]\beta[q]} P_3$  to represent multi-step transition.

**Probabilistic Bisimulation:** We recall the definition of cumulative probability distribution function (cPDF) [22] which computes the total probability in which a process derives a set of processes.  $\wp$  is the powerset operator and we write  $\mathbf{Pr}/\mathcal{R}$  to denote the set of equivalence classes induced by equivalence relation  $\mathcal{R}$  over  $\mathbf{Pr}$ .

**DEFINITION 2.1.**  $\mu : (\mathbf{Pr} \times \mathbf{Act} \times \wp(\mathbf{Pr})) \rightarrow [0, 1]$  is the total function given by:  $\forall \alpha \in \mathbf{Act}$ ,  $\forall P \in \mathbf{Pr}$ ,  $\forall C \subseteq \mathbf{Pr}$ ,  $\mu(P, \alpha, C) = \sum \{p | P \xrightarrow{\alpha[p]} Q, Q \in C\}$ .

**DEFINITION 2.2.** An equivalence relation  $\mathcal{R} \subseteq \mathbf{Pr} \times \mathbf{Pr}$  is a *probabilistic bisimulation* if  $(P, Q) \in \mathcal{R}$  implies:  $\forall C \in \mathbf{Pr}/\mathcal{R}$ ,  $\forall \alpha \in \mathbf{Act}$ ,  $\mu(P, \alpha, C) = \mu(Q, \alpha, C)$ .

$P$  and  $Q$  are probabilistic bisimilar, written as  $P \sim Q$ , if there exists a probabilistic bisimulation  $\mathcal{R}$  s.t.  $PRQ$ .

## 2.3 Modelling for Network Security based on PVCCS<sub>R</sub>

**ComModel** focuses on modeling the network security scenario modeled usually via perfect and complete information game: a network system state considers the situations of attacker, defender and network environment together; the participants act in turn at each state and the interactions among the participants will cause the network state transition with certain probability; each state transition produces immediate payoff to attacker and defender, and the former (positive values) is in terms of the extent of damage he does to the network while the latter (negative values) is measured by the time of recovery; the future offensive-defensive behaviors will impact on the action choice of attacker and defender at each state. Nash Equilibrium strategy represents a stable plan of action for attacker and defender in long run, while the Social Optimal strategy is a policy to minimize the damage caused by attacker.

Assuming  $S$  is the set of network system state, ranged over by  $s_i$ ,  $i \in I$ ,  $I$  is an index set; action sets of attacker and defender are  $A^a$  and  $A^d$  respectively,  $u, v$  represent the general values,  $A^a(s_i) \subseteq A^a$  is the action set of attacker at  $s_i$ , as well as  $A^d(s_i) \subseteq A^d$  is that of defender; state transition probability is a function  $\dot{p} : S \times A^a \times A^d \times S \rightarrow [0, 1]$ , and immediate payoff associated with each transition is a function  $\dot{r} : S \times A^a \times A^d \rightarrow \mathbb{R}_1 \times \mathbb{R}_2$ , where  $\mathbb{R}$  is the real number set, and we use index to distinguish the first and the second element, and  $\dot{r}^a : S \times A^a \times A^d \rightarrow \mathbb{R}_1$  represents the immediate payoff of attacker, while  $\dot{r}^d : S \times A^a \times A^d \rightarrow \mathbb{R}_2$  is that of defender.

**ComModel**, a model based on PVCCS<sub>R</sub>, is used to modeling for the network security scenario depicted as above. The processes represent all possible behaviors of the participants in network system at each state. Each state is assigned with a process depicting all possible interactions currently performed among the participants. Then we establish a network state transition system based on the process transitions.

In **ComModel**, the channel set  $\mathcal{A} = \{Attc, Defd, Tell_a, Tell_d\}$ ,  $\mathbf{Label} = \mathcal{A} \cup \bar{\mathcal{A}} \cup \{\overline{Log}\} \cup \{\overline{Rec}\}$ . The value set  $\mathbf{Val} = A^a \cup A^d \cup T$ , where  $T \subseteq \mathbb{R} \times \mathbb{R}$ . **Var** is the set of value variables. **Act** is the union of behavior sets of the three participants ( $Act^a, Act^d$  and  $Act^n$ ) defined as follows:

$$\begin{aligned} \mathbf{Act} &= Act^a \cup Act^d \cup Act^n \\ Act^a &= \{\overline{Attc}(v) \mid v \in A^a\} \cup \{Tell_a(x) \mid x \in \mathbf{Var}\} \\ Act^d &= \{\overline{Defd}(v) \mid v \in A^d\} \cup \{Tell_d(x) \mid x \in \mathbf{Var}\} \\ Act^n &= \{Attc(x) \mid x \in \mathbf{Var}\} \cup \{Defd(x) \mid x \in \mathbf{Var}\} \\ &\quad \cup \{\overline{Tell_a}(x) \mid x \in \mathbf{Var} \cup A^d\} \\ &\quad \cup \{\overline{Tell_d}(x) \mid x \in \mathbf{Var} \cup A^a\} \\ &\quad \cup \{\overline{Log}(x, y) \mid x \in A^a \cup \mathbf{Var}, y \in A^d \cup \mathbf{Var}\} \\ &\quad \cup \{\overline{Rec}(\dot{r}(s, u, v)) \mid s \in S, u \in A^a, v \in A^d\} \end{aligned}$$

Figure 2 shows one interaction among the participants at state  $s$ .  $\overline{Attc}(u)$  means attacker takes attack  $u$ , similar to  $\overline{Defd}(v)$  for defender;  $Attc(x)$  (or  $Defd(x)$ ) means network environment is attacked (or is defended);  $Tell_d(x)$  (or  $Tell_a(x)$ ) means network environment informs defender (or attacker) the action chosen by attacker (or defender);  $Tell_d(x)$  (or  $Tell_a(x)$ ) means defender (or attacker) is informed that

$[In] \frac{}{\sum_{i \in I} \sum_{j \in J} [p_{ij}] a(x). P_{ij} \xrightarrow{a(e)[p_{ij}]} P_{ij}\{e/x\}}$	$[Out] \frac{}{\sum_{i \in I} \sum_{j \in J} [p_{ij}] \bar{a}(e). P_{ij} \xrightarrow{\bar{a}(e)[p_{ij}]} P_{ij}}$
$[Res] \frac{P \xrightarrow{\alpha[p]} P'}{P \setminus R \xrightarrow{\alpha[p]} P' \setminus R} \quad (chan(\alpha) \notin R \cup \bar{R})$	$[Con] \frac{P\{e/x\} \xrightarrow{\alpha[p]} P'}{A(e) \xrightarrow{\alpha[p]} P'} \quad (A(x) \stackrel{def}{=} P)$
$[Par_l] \frac{P_1 \xrightarrow{\alpha[p]} P'_1}{P_1   P_2 \xrightarrow{\alpha[p]} P'_1   P_2}$	$[Par_r] \frac{P_2 \xrightarrow{\alpha[p]} P'_2}{P_1   P_2 \xrightarrow{\alpha[p]} P_1   P'_2}$
$[Com] \frac{P_1 \xrightarrow{a(e)[p]} P'_1, P_2 \xrightarrow{\bar{a}(e)[q]} P'_2}{P_1   P_2 \xrightarrow{\tau[p,q]} P'_1   P'_2}$	
$[If_t] \frac{P_1 \xrightarrow{\alpha[p]} P'_1}{if \mathbf{b} \text{ then } P_1 \text{ else } P_2 \xrightarrow{\alpha[p]} P'_1} \quad (\mathbf{b} = true)$	$[If_f] \frac{P_2 \xrightarrow{\alpha[p]} P'_2}{if \mathbf{b} \text{ then } P_1 \text{ else } P_2 \xrightarrow{\alpha[p]} P'_2} \quad (\mathbf{b} = false)$

Table 1: Operational semantics of PVCCS<sub>R</sub>

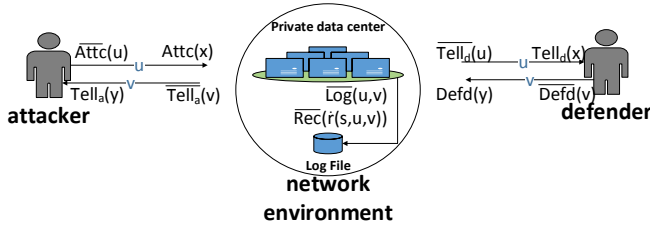


Figure 2: Interactions among participants at state  $s$

attack (or defense) has happened;  $\overline{Log}(x, y)$  means the network environment writes the values of  $x$  and  $y$  into a log file, where  $x$  and  $y$  is used to receive the values of attack and defense respectively;  $\overline{Rec}(\dot{r}(s, u, v))$  stands for the network environment records the immediate payoff to attacker and defender if they choose  $u$  and  $v$  at state  $s$  respectively.

The processes describing all possible behaviors of the participants at state  $s_i$ , denoted by  $pA_i$ ,  $pD_i$  and  $pN_i$ , are defined as follows:

$$\begin{aligned}
pA_i &\stackrel{def}{=} \sum_{u \in A^a(s_i)} \overline{Attc}(u). \overline{Tell}_a(y). Nil \\
pD_i &\stackrel{def}{=} \overline{Tell}_d(x). \sum_{v \in A^d(s_i)} \overline{Defd}(v). Nil \\
pN_i &\stackrel{def}{=} \overline{Attc}(x). \overline{Tell}_d(x). \overline{Defd}(y). \overline{Tell}_a(y). Tr_i(x, y) \\
Tr_i(x, y) &\stackrel{def}{=} \sum_{\substack{u \in A^a(s_i) \\ v \in A^d(s_i)}} \overline{Log}(u, v). (if (x = u, y = v) \text{ then} \\
&\quad \sum_{j \in I} [\dot{p}(s_i, u, v, s_j)] \overline{Rec}(\dot{r}(s_i, u, v)). (pA_j | pD_j | pN_j) \\
&\quad \text{else Nil})
\end{aligned}$$

The process assigned to each state  $s_i$  is defined as

$$G_i \stackrel{def}{=} (pA_i | pD_i | pN_i) \setminus R, R = \{\overline{Attc}, \overline{Defd}, \overline{Tell}_a, \overline{Tell}_d\}$$

We get the network state transition system, **TS** for short, based on process transitions. Minimizing **TS** by shrinking probabilistic bisimilar pairs of states. We conduct a series of

path contractions on **TS** and obtained a new graph named as **ConTS** without information loss as follows:

DEFINITION 2.3. **ConTS** is a tuple  $(V, E, L)$

- $V = \{G_i \mid G_i \text{ is the process we assign to state } s_i\}$
- $E = \{(G_i, G_j) \mid \text{ranged over } e_{ij}, \text{ if there exists a multi-transition } G_i \xrightarrow{(\tau[1])^4 \overline{Log}(u, v)[1] \overline{Rec}(\dot{r}(s_i, u, v))[\dot{p}(s_i, u, v, s_j)]} G_j\}$
- $L(e_{ij}) = \{(L_{Act}(e_{ij}), L_{TranP}(e_{ij}), L_{WeiP}(e_{ij}) \mid e_{ij} \in E\}$ 
  - action pair:  $L_{Act}(e_{ij}) = (u, v)$
  - \*  $L_{Act}^a(e_{ij}) = u, L_{Act}^d(e_{ij}) = v$
  - transition probability:  $L_{TranP}(e_{ij}) = \dot{p}(s_i, u, v, s_j)$
  - weight pair:  $L_{WeiP}(e_{ij}) = \dot{r}(s_i, u, v)$
  - \*  $L_{WeiP}^a(e_{ij}) = \dot{r}^a(s_i, u, v)$
  - \*  $L_{WeiP}^d(e_{ij}) = \dot{r}^d(s_i, u, v)$

$L_{WeiP}^S(e_{ij}) = L_{WeiP}^a(e_{ij}) + |L_{WeiP}^d(e_{ij})|$  denotes the sum of absolute weight pair of  $e_{ij}$ . By convention, in any network security scenario, for any  $e, e' \in E$ , if  $L_{WeiP}^a(e) > L_{WeiP}^a(e')$  then  $L_{WeiP}^d(e) < L_{WeiP}^d(e')$ .

### 3. ANALYZING PROPERTIES AS GRAPH THEORY APPROACH

We firstly introduce the definitions of Nash Equilibrium strategy (*NES*) and Social Optimal strategy (*SOS*) in our model, and then we illustrate the algorithms proposed to compute *NES* and *SOS* respectively.

#### 3.1 NES and SOS

DEFINITION 3.1.  $\forall G_i \in V$ , an execution of  $G_i$  in **ConTS**, denoted by  $\pi_i$ , is a walk (vertices and edges appearing alternately) starting from  $G_i$  and ending with a cycle, on which every vertex's out-degree is 1.

According to the definition of execution,  $\pi_i$  is in the form of  $G_i e_{ij} G_j \dots (G_k \dots G_l e_{lk} G_k)$  which is ended by a cycle starting with  $G_k$ , where  $G_i$  and  $G_k$  may be the same node.  $\pi_i$  can be written as  $\pi_i^e$  if  $e$  is the first edge of  $\pi_i$ ;  $\pi_i[j]$  denotes the subsequence of  $\pi_i$  starting from  $G_j$ , where  $G_j$  is a vertex on  $\pi_i$ .

DEFINITION 3.2. The *payoff* to attacker and defender on execution  $\pi_i$ , denoted by  $PF^a(\pi_i)$  and  $PF^d(\pi_i)$  respectively, are defined as follows:

$$PF^a(\pi_i) = L_{Weip}^a(e_{ij}) + \beta \cdot L_{TranP}(e_{ij}) \cdot PF^a(\pi_i[j])$$

$$PF^d(\pi_i) = L_{Weip}^d(e_{ij}) + \beta \cdot L_{TranP}(e_{ij}) \cdot PF^d(\pi_i[j])$$

where  $\beta \in (0, 1)$  is a discount factor. The sum of absolute payoff on  $\pi_i$  of attacker and defender is denoted as  $PF^S(\pi_i)$ , and  $PF^S(\pi_i) = PF^a(\pi_i) + |PF^d(\pi_i)|$ .

THEOREM 3.1.  $\forall G_i \in V$ ,  $\pi_i$  is an execution of  $G_i$ ,  $PF^a(\pi_i)$  and  $PF^d(\pi_i)$  are converged.

PROOF. Based on the definition of payoff on an execution of  $G_i$  and limiting laws, we show the proof details for  $PF^a(\pi_i)$  in Appendix. The proof for  $PF^d(\pi_i)$  is similar.  $\square$

Nash Equilibrium Execution and Social Optimal Execution are defined coinductively [18] as follows:

DEFINITION 3.3.  $\pi_i$  is *Nash Equilibrium Execution (NEE)* of  $G_i$  if it satisfies:

$$PF^a(\pi_i) = \max_{e_{ij} \in E'(G_i)} \{L_{Weip}^a(e_{ij}) + \beta \cdot L_{TranP}(e_{ij}) \cdot PF^a(\pi_j)\}$$

$$PF^d(\pi_i) = \max_{e_{ij} \in E_e^d(G_i)} \{L_{Weip}^d(e_{ij}) + \beta \cdot L_{TranP}(e_{ij}) \cdot PF^d(\pi_j)\}$$

where  $\pi_j$  is NEE of  $G_j$ ,  $e$  is the first edge of  $\pi_i$ ,  $E_e^a(G_i) = \{e' \in E(G_i) \mid L_{Act}^a(e') = L_{Act}^a(e)\}$  including  $e$ , and  $E'(G_i) = \{\arg \max_{e' \in E_{e''}^a(G_i)} \{L_{Weip}^d(e') + \beta \cdot L_{TranP}(e') \cdot PF^d(\pi_j)\}, \forall e'' \in E(G_i)\}$ .

DEFINITION 3.4.  $\pi_i$  is *Social Optimal Execution (SOE)* of  $G_i$ , if it satisfies:

$$PF^S(\pi_i) = \min_{e_{ij} \in E(G_i)} \{L_{Weip}^S(e_{ij}) + \beta \cdot L_{TranP}(e_{ij}) \cdot PF^S(\pi_j)\}$$

where  $\pi_j$  is SOE of  $G_j$

DEFINITION 3.5. *Strategy* is a sequence consisting of action pair (one from attacker and one from defender) at each state.

DEFINITION 3.6. *Nash Equilibrium Strategy (NES)* is a strategy of which every  $G_i$ 's execution based on is NEE of  $G_i$ .

DEFINITION 3.7. *Social Optimal Strategy (SOS)* is a strategy of which every  $G_i$ 's execution based on is SOE of  $G_i$ .

## 3.2 Algorithms

The way to compute *NES* (or *SOS*) in **ConTS** is to find a spanning subgraph of **ConTS** satisfying following conditions:

- A. Each vertex's outdegree is 1;
- B. Each vertex's execution in this subgraph is its *NEE* (or *SOE*).

For backward inductive analysis, we firstly find SCC of **ConTS** based on Tarjan's algorithm [5] and construct **Abstraction (Abs)** for short) by viewing each SCC as one vertex.  $V(\mathbf{Abs})$  denotes the vertex set of **Abs** ranged over by  $D$ . **Abs** is a DAG, and we rename  $D$  with *Leave* if its out-degree is 0, else with *Non-Leave*. By convention,  $\forall D \in V(\mathbf{Abs})$ ,  $V(D) = \{G_i \in V \mid G_i \text{ belongs to the SCC represented by } D\}$ .

DEFINITION 3.8.  $\forall D \in V(\mathbf{Abs})$ , the *priority* of  $D$ , denoted by  $prior(D)$ , is defined inductively:

(1)  $prior(D) = n$ , if  $D$  is a *Leave*, and  $n$  is the size of  $V(\mathbf{Abs})$ .

(2)  $prior(D) = \min\{prior(D') - 1 \mid D' \text{ is any direct successor of } D \text{ in } \mathbf{Abs}\}$

DEFINITION 3.9.  $D$  *depends on*  $D'$  if  $D'$  appears in one of the paths starting from  $D$  in **Abs**.

THEOREM 3.2. If  $prior(D) < prior(D')$  then  $D'$  does not depend on  $D$ .

PROOF. We prove it by contradiction: if  $D'$  depends on  $D$ , then  $D$  appears in one of the paths starting from  $D'$  in **Abs**, so we have  $prior(D') = \min\{prior(D'') - 1 \mid D'' \text{ is any direct successor of } D' \text{ in } \mathbf{Abs}\} < prior(D)$ , contradiction.  $\square$

If  $D$  does not depend on  $D'$ , then computing *NES/SOS* of  $D'$  has no impact on computing *NES/SOS* of  $D$ . To find *NES/SOS* of  $D$  is to find *NEE/SOE* of all  $G_i \in V(D)$ .

The algorithms for computing *NES* and *SOS*, denoted as **AlgNES()** and **AlgSOS()** respectively, are both based on backward induction. The framework of **AlgNES()** is as follows:

- (1) Compute priority of each vertex  $D$  in **Abs**;
- (2) Compute *NES* for *Leave* firstly, then compute backward inductively for *Non-Leave*.

The framework of **AlgSOS()** is similar.

Pseudo code of **AlgNES()** is shown in Algorithm 1.

```

Data: Abs
Result: NES of Abs
NES(Abs)  $\leftarrow \emptyset$ ;
for  $D \in V(\mathbf{Abs})$  do
  |  $prior(D) \leftarrow \text{ComputePrior}(D)$ ;
end
List  $\mathcal{L} \leftarrow$  list of  $V(\mathbf{Abs})$  in descending order on priority;
pointer  $p \leftarrow \mathcal{L}$ ;
while  $p$  is not the tail of  $\mathcal{L}$  do
  |  $D \leftarrow p.data$ ;
  | while  $prior(D)$  is the highest in  $\mathcal{L}$  do
    |  $NES(\mathbf{Abs}) \cup \leftarrow NESinLeave(D)$ ;
    |  $p \leftarrow p.next$ ;
    |  $D \leftarrow p.data$ ;
  | end
  |  $NES(\mathbf{Abs}) \cup \leftarrow NESinNonLeave(D)$ ;
  |  $p \leftarrow p.next$ ;
  |  $D \leftarrow p.data$ ;
end

```

Algorithm 1: Pseudo code of **AlgNES()**

## NES/SOS for Leave

The key point of computing *NES* (or *SOS*) for *Leave D* is to find a cycle in *D* satisfying conditions **A** and **B** as above.

**NES in Leave:** The method of finding *NES* for *Leave D* is a value iteration method, denoted as **NESinLeave**(*D*). The value function is **BackInd**(*G<sub>i</sub>*) which returns some edge *e* of *G<sub>i</sub>* and **RefN**(*G<sub>i</sub>*) is used to refresh the value of the weight pair for each edge of *G<sub>i</sub>*,  $\forall G_i \in \mathcal{V}(D)$ .

As the narrative convenience, we introduce some auxiliary symbols:  $\forall e \in E(G_i)$ , the weight pair initializes with  $L_0(e) = L_{Weip}(e)$ , and  $L_n(e) = (L_n^a(e), L_n^d(e))$  is used to keep the new weight pair of *e* obtained by **RefN**(*G<sub>i</sub>*) on the *n*th iteration;  $\forall G_i \in \mathcal{V}(D)$ ,  $Pp_n(G_i) = (Pp_n^a(G_i), Pp_n^d(G_i))$ , initialized with  $Pp_0(G_i) = (0, 0)$ , is used to keep  $L_n(e)$ , where *e* is the result of **BackInd**(*G<sub>i</sub>*) on the *n*th iteration. The iterative process will be continued until  $\forall G_i \in \mathcal{V}(D)$ ,  $Pp_n(G_i) = Pp_{n+1}(G_i)$ .

The framework of **NESinLeave**(*D*) is as follows:

- (1) Value iteration initializes with **BackInd**(*G<sub>i</sub>*), where for each  $G_i \in \mathcal{V}(D)$ , the weight pair of  $e \in E(G_i)$  is  $L_0(e)$ . Assuming *e* is the result obtained by **BackInd**(*G<sub>i</sub>*), then  $Pp_0(G_i) = L_0(e)$ ;
- (2) Loops through the method **RefN**(*G<sub>i</sub>*) and **BackInd**(*G<sub>i</sub>*) by order until  $\forall G_i$ ,  $Pp_{n+1}(G_i) = Pp_n(G_i)$ ;
- (3)  $\forall G_i$ , execute **BackInd**(*G<sub>i</sub>*). The cycle obtained is what we want.

Rules of method **BackInd**(*G<sub>i</sub>*) on the *n*th iteration,  $n \geq 0$ :

- (1) Let  $E' = E(G_i)$ ;
- (2) If  $\exists e_1, e_2 \in E'$  satisfying  $L_{Act}^a(e_1) = L_{Act}^a(e_2)$ , refresh  $E'$  by filtering the edge  $e \neq \arg \max_{e \in \{e_1, e_2\}} L_n^d(e)$ ;
- (3) Refresh  $E'$  by keeping edge  $e = \arg \max_{e \in E'} L_n^a(e)$ ;
- (4) Return *e*.

Rules in method **RefN**(*G<sub>i</sub>*) on the (*n*+1)th iteration,  $n \geq 0$ :

- (1)  $\forall e \in E(G_i)$ , compute its  $L_{n+1}(e)$  componentwise by following formula:

$$L_{n+1}(e_{ij}) = L_{Weip}(e_{ij}) + \beta \cdot L_{TranP}(e_{ij}) \cdot Pp_n(G_j)$$

- (2) Keep  $L_{n+1}(e_{ij})$ ,  $\forall e_{ij} \in E(G_i)$ ;

Pseudo code of **NESinLeave**(), **BackInd**() and **RefN**() are shown in Algorithm 2, 3 and 4 respectively.

**Data:** *Leave of Abs: D*

**Result:** *NES of D*

Label  $G_i \in \mathcal{V}(D)$  with **NonConducted**;

$NES(D) \leftarrow \emptyset$ ;

**while**  $\exists G_i$  is **NonConducted** **do**

$e \leftarrow \text{BackInd}(G_i)$ ;

$Pp_0(G_i) \leftarrow L_0(e)$ ;

    Label  $G_i$  with **Conducted**;

**end**

**while**  $\exists G_i$   $Pp_n(G_i) \neq Pp_{n+1}(G_i)$  componentwise **do**

**RefN**(*G<sub>i</sub>*) ;

$e \leftarrow \text{BackInd}(G_i)$ ;

$Pp_{n+1}(G_i) \leftarrow L_{n+1}(e)$ ;

**end**

$NES(D) \leftarrow \{e | e \leftarrow \text{BackInd}(G_i), G_i \in \mathcal{V}(D)\}$ ;

**Algorithm 2:** Pseudo code of **NESinLeave**()

**Data:**  $G_i \in \mathcal{V}(D)$

**Result:** edge  $e \in E(G_i)$

create  $E' \leftarrow E(G_i)$ ;

**while**  $\forall e_1, e_2 \in E'$  with  $L_{Act}^a(e_1) = L_{Act}^a(e_2)$  **do**  
     $E' \leftarrow E' \setminus \{e \mid e \neq \arg \max_{e \in \{e_1, e_2\}} L_n^d(e)\}$ ;

**end**

$e \leftarrow \arg \max_{e \in E'} L_n^a(e)$ ;

return *e*;

**Algorithm 3:** Pseudo code of **BackInd**()

**Data:**  $G_i \in \mathcal{V}(D)$

**Result:**  $L_{n+1}(e_{ij})$ ,  $\forall e_{ij} \in E(G_i)$

Label all  $e_{ij} \in E(G_i)$  with **NonRef**;

**while**  $\exists e_{ij}$  is **NonRef** **do**

$L_{n+1}^a(e_{ij}) \leftarrow L_{Weip}^a(e_{ij}) + \beta \cdot L_{TranP}(e_{ij}) \cdot Pp_n^a(G_j)$ ;

$L_{n+1}^d(e_{ij}) \leftarrow L_{Weip}^d(e_{ij}) + \beta \cdot L_{TranP}(e_{ij}) \cdot Pp_n^d(G_j)$ ;

    Label  $e_{ij}$  with **Ref**;

**end**

**Algorithm 4:** Pseudo code of **RefN**()

**SOS in Leave:** The method **SOSinLeave**(*D*) used to find *SOS* for *Leave D* is also a value iteration method. The *value function* is **LocSoOp**(*G<sub>i</sub>*) which returns some edge *e* of *G<sub>i</sub>* and **RefS**(*G<sub>i</sub>*) is used to refresh the absolute sum value of the weight pair for each edge of *G<sub>i</sub>*,  $\forall G_i \in \mathcal{V}(D)$ .

Here are some other auxiliary symbols for convenience:  $\forall e \in E(G_i)$ , its sum of absolute weight pair initializes with  $L_0^S(e) = L_{Weip}^S(e)$ , and  $L_n^S(e)$  is used to keep the new sum of absolute weight pair of *e* obtained by **RefS**(*G<sub>i</sub>*) on the *n*th iteration;  $Pp_n(G_i)$  initialized with  $Pp_0(G_i) = 0$ , is used to keep  $L_n^S(e)$ , where *e* is the result of **LocSoOp**(*G<sub>i</sub>*) on the *n*th iteration. The iterative process will be continued until  $\forall G_i \in \mathcal{V}(D)$ ,  $Pp_n(G_i) = Pp_{n+1}(G_i)$ .

The framework of **SOSinLeave**(*D*) is as follows:

- (1) Value iteration initializes with **LocSoOp**(*G<sub>i</sub>*), where for  $G_i \in \mathcal{V}(D)$ , the sum of absolute weight pair of  $e \in E(G_i)$  is  $L_0^S(e)$ . Assuming the result obtained by **LocSoOp**(*G<sub>i</sub>*) is *e*, then  $Pp_0(G_i) = L_0^S(e)$ ;
- (2) Loops through the method **RefS**(*G<sub>i</sub>*) and **LocSoOp**(*G<sub>i</sub>*) by order until  $\forall G_i$ ,  $Pp_{n+1}(G_i) = Pp_n(G_i)$ ;
- (3)  $\forall G_i$ , execute **LocSoOp**(*G<sub>i</sub>*). The cycle obtained is what we want.

Rules of method **LocSoOp**(*G<sub>i</sub>*) on *n*th iteration,  $n \geq 0$ :

- (1) Compare  $L_n^S(e)$ ,  $\forall e \in E(G_i)$ ;
- (2) Return edge  $e = \arg \min_{e \in E(G_i)} \{L_n^S(e)\}$ .

Rules of method **RefS**(*G<sub>i</sub>*) on (*n*+1)th iteration,  $n \geq 0$ :

- (1)  $\forall e_{ij} \in E(G_i)$ , compute its  $L_{n+1}^S(e_{ij})$  by following formula:

$$L_{n+1}^S(e_{ij}) = L_{Weip}^S(e_{ij}) + \beta \cdot L_{TranP}(e_{ij}) \cdot Pp_n(G_j)$$

- (2) Keep  $L_{n+1}^S(e_{ij})$ ,  $\forall e \in E(G_i)$ ;

Pseudo code of **SOSinLeave**(), **LocSoOp**() and **RefS**() are given in Algorithm 5, 6 and 7 respectively.

## NES/SOS for Non-Leave

**NES of Non-Leave:** For *Non-Leave* vertex *D* in **Abs**, the method of computing its NES is **NESinNonLeave**(*D*) and its framework is as follows:

**Data:** *Leave* of **Abs**:  $D$   
**Result:** *SOS* of  $D$   
Label  $G_i \in \mathcal{V}(D)$  with **NonConducted**;  
 $SOS(D) \leftarrow \emptyset$ ;  
**while**  $\exists G_i$  is **NonConducted** **do**  
     $e \leftarrow \text{LocSoOp}(G_i)$ ;  
     $Ps_0(G_i) \leftarrow L_0^S(e)$ ;  
    Label  $G_i$  with **Conducted**;  
**end**  
**while**  $\exists G_i Ps_n(G_i) \neq Ps_{n+1}(G_i)$  **do**  
    **RefS**( $G_i$ ) ;  
     $e \leftarrow \text{LocSoOp}(G_i)$ ;  
     $Ps_{n+1}(G_i) \leftarrow L_{n+1}^S(e)$ ;  
**end**  
 $SOS(D) \leftarrow \{e | e \leftarrow \text{LocSoOp}(G_i), G_i \in \mathcal{V}(D)\}$ ;

**Algorithm 5:** Pseudo code of **SOSinLeave**()

**Data:**  $G_i \in \mathcal{V}(D)$   
**Result:** edge  $e \in E(G_i)$   
**while**  $\exists e \in E(G_i)$  is not compared **do**  
     $e' \leftarrow \arg \min_{e \in E} \{L_n^S(e)\}$ ;  
**end**  
return  $e'$ ;

**Algorithm 6:** Pseudo code of **LocSoOp**()

**Data:**  $G_i \in \mathcal{V}(D)$   
**Result:**  $L_{n+1}^S(e_{ij}), \forall e_{ij} \in E(G_i)$   
Label all  $e_{ij} \in G_i$  with **NonRef**;  
**while**  $\exists e_{ij}$  is **NonRef** **do**  
     $L_{n+1}^S(e_{ij}) \leftarrow L_{WeiP}^S(e_{ij}) + \beta \cdot L_{TranP}(e_{ij}) \cdot Ps_n(G_j)$ ;  
    Label  $e_{ij}$  with **Ref**;  
**end**

**Algorithm 7:** Pseudo code of **RefS**()

- (1) if the size of  $\mathcal{V}(D)$  is more than 1, we will pre-process  $D$  with method **PrePro**( $D$ ) firstly, then get its *NES* by **NESinLeave**( $D$ );
- (2) if  $\mathcal{V}(D) = \{G_i\}$  for some  $G_i \in V$ , then the *NES* of  $D$  is the result obtained from **BackInd**( $G_i$ ) directly.

Rules in method **PrePro**( $D$ ) are as follows:

- (1)  $D'$  is one direct successor of  $D$  in **Abs**, and if the edge  $e$  connecting  $D$  and  $D'$  is contributed by the connection between  $G_i \in \mathcal{V}(D)$  and  $G_j \in \mathcal{V}(D')$ , then  $L_0(e_{ij}) = L_{WeiP}(e_{ij}) + \beta \cdot L_{TranP}(e_{ij}) \cdot PF(\pi_j)$  componentwise, where  $\pi_j$  is the nash equilibrium execution of  $G_j$ ;
- (2) Change  $e$  to be the self-loop edge of  $G_i$ .

Pseudo code of **NESinNonLeave**() and **PrePro**() are shown in Algorithm 8 and Algorithm 9 respectively.

**Data:** *Non-Leave*:  $D$   
**Result:** *NES* of  $D$   
 $NES(D) \leftarrow \emptyset$ ;  
**if** the size of  $\mathcal{V}(D)$  is bigger than 1 **then**  
     $D' \leftarrow \text{PrePro}(D)$ ;  
     $NES(D) \leftarrow \text{NESinLeave}(D')$ ;  
**else**  
     $NES(D) \leftarrow \text{BackInd}(G_i)$ , if  $\mathcal{V}(D) = \{G_i\}$ ;  
**end**

**Algorithm 8:** Pseudo code of **NESinNonLeave**()

**SOS of Non-Leave:** The method **SOSinNonLeave**( $D$ ) computing *SOS* for *Non-Leave*  $D$  is identical to **NESinNonLeave**( $D$ ) except for the preprocessing method **PreProS**( $D$ ). The computing steps of **PreProS**( $D$ ) are as fol-

**Data:** *Non-Leave*:  $D$   
**Result:** new  $D'$   
 $E' \leftarrow E(G_i), G_i \in \mathcal{V}(D)$ ;  
**while**  $\exists e_{ij} \in E'$  with endpoint  $G_j \notin \mathcal{V}(D)$  **do**  
     $L_0^a(e_{ij}) \leftarrow L_{WeiP}^a(e_{ij}) + \beta \cdot L_{TranP}(e_{ij}) \cdot Pp^a(G_j)$ ;  
     $L_0^d(e_{ij}) \leftarrow L_{WeiP}^d(e_{ij}) + \beta \cdot L_{TranP}(e_{ij}) \cdot Pp^d(G_j)$ ;  
    Change  $e_{ij}$  to be self-loop edge of  $G_i$ ;  
**end**  
 $D' \leftarrow (\mathcal{V}(D), E')$ ;  
Return  $D'$ ;

**Algorithm 9:** Pseudo code of **PrePro**()

lows:

- (1)  $D'$  is one direct successor of  $D$  in **Abs**, if the edge  $e$  connecting  $D$  and  $D'$  is contributed by connection between  $G_i \in \mathcal{V}(D)$  and  $G_j \in \mathcal{V}(D')$ , then  $L_0^S(e_{ij}) = L_{WeiP}^S(e_{ij}) + \beta \cdot L_{TranP}(e_{ij}) \cdot PF^S(\pi_j)$ , where  $\pi_j$  is social optimal execution of  $G_j$ ;
- (2) Change  $e$  to be self-loop edge of  $G_i$ .

Pseudo code of **SOSinNonLeave**() and **PreProS**() is shown in Algorithm 10 and Algorithm 11 respectively in Appendix.

**Data:** *Non-Leave*:  $D$   
**Result:** *SOS* of  $D$   
 $SOS(D) \leftarrow \emptyset$ ;  
**if** the size of  $\mathcal{V}(D)$  is bigger than 1 **then**  
     $D' \leftarrow \text{PreProS}(D)$ ;  
     $SOS(D) \leftarrow \text{SOSinLeave}(D')$ ;  
**else**  
     $SOS(D) \leftarrow \text{LocSoOp}(G_i)$ , if  $\mathcal{V}(D) = \{G_i\}$ ;  
**end**

**Algorithm 10:** Pseudo code of **SOSinNonLeave**()

**Data:** *Non-Leave*:  $D$   
**Result:** new  $D'$   
 $E' \leftarrow E(G_i), G_i \in \mathcal{V}(D)$ ;  
**while**  $\exists e_{ij} \in E'$  with endpoint  $G_j \notin \mathcal{V}(D)$  **do**  
     $L_0^S(e_{ij}) \leftarrow L_{WeiP}^S(e_{ij}) + \beta \cdot L_{TranP}(e_{ij}) \cdot Ps(G_j)$ ;  
    Change  $e_{ij}$  to be self-loop edge of  $G_i$ ;  
**end**  
 $D' \leftarrow (\mathcal{V}(D), E')$ ;  
Return  $D'$ ;

**Algorithm 11:** Pseudo code of **PreProS**()

### 3.3 Correctness of Algorithms

#### Correctness of **NESinLeave**()

Inspired by a technique in dynamic programming which is called *value-iteration* [23, 20], **BackInd**( $D$ ) is formalized as a mapping  $\sigma : \mathcal{V}(D) \rightarrow \mathbb{R} \times \mathbb{R}$ , on  $k$ th iteration,  $\sigma_k(G_i) = (\sigma_k(G_i)^a, \sigma_k(G_i)^d) = Pp_k(G_i)$ . **RefN**() defines a set of vertex  $\{G_i(\sigma_k) \mid G_i(\sigma_k) \text{ denotes } G_i \text{ with } e_{ij} \text{ whose weight pair is refreshed by the rule componentwise: } L_{k+1}(e_{ij}) = L_{WeiP}(e_{ij}) + \beta \cdot L_{TranP}(e_{ij}) \cdot \sigma_k(G_j)\}$ . According to the rules of **NESinLeave**( $D$ ),  $\sigma_{k+1}(G_i) = Pp_1(G_i(\sigma_k))$  for any  $G_i \in \mathcal{V}(D)$ . It is convenient to define the shorthand operator notation  $(T\sigma)(G_i) = Pp_1(G_i(\sigma))$ , that is  $T\sigma_k = \sigma_{k+1}$ .

LEMMA 3.1. For any  $G_i \in \mathcal{V}(D)$ , we have

$$|\sigma_k(G_i)^a - T\sigma_k(G_i)^a| \leq \max_{e \in E(G_i)} |L_k^a(e) - L_{k+1}^a(e)|$$

$$|\sigma_k(G_i)^d - T\sigma_k(G_i)^d| \leq \max_{e \in E(G_i)} |L_k^d(e) - L_{k+1}^d(e)|$$

PROOF. We prove by contradiction for the first inequality in details. According to the rules in **BackInd**( $G_i$ ), we need to consider all possible results obtained by **BackInd**( $G_i$ ) on  $k$ th and  $(k+1)$ th iteration respectively. The details are shown in Appendix. The proof for the second inequality is similar.  $\square$

LEMMA 3.2.  $T$  is a contraction.

PROOF. For any real vector  $\vec{x} \in \mathbb{R}^J$ ,  $J$  is an index set, let  $\|\vec{x}\|_\infty = \max_j |x_j|$ . According to Lemma 3.1, then we have

$$\begin{aligned} \|T\sigma_{k+1}^a - T\sigma_k^a\|_\infty &= \max_{G_i \in V} |T\sigma_{k+1}(G_i)^a - T\sigma_k(G_i)^a| \\ &\leq \max_{G_i \in V} \max_{e_{ij} \in E(G_i)} |L_{k+2}^a(e_{ij}) - L_{k+1}^a(e_{ij})| \\ &\leq \max_{G_j \in V} \beta \cdot |\sigma_{k+1}(G_j)^a - \sigma_k(G_j)^a| \\ &= \beta \cdot \|\sigma_{k+1}^a - \sigma_k^a\|_\infty \end{aligned}$$

similar proof for  $\|T\sigma_{k+1}^d - T\sigma_k^d\|_\infty \leq \beta \cdot \|\sigma_{k+1}^d - \sigma_k^d\|_\infty$ . Therefore, we claim that  $\exists \sigma_*$ , satisfying  $T\sigma_* = \sigma_*$ .  $\square$

THEOREM 3.3. If  $D$  is a Leave of **Abs**, then the result obtained by **NESinLeave**( $D$ ) is NES of  $D$ .

PROOF. We need to prove two issues:

1. **NESinLeave**( $D$ ) is terminated.
  2. The execution of  $G_i$ ,  $\forall G_i \in \mathcal{V}(D)$ , based on the result of **NESinLeave**( $D$ ) is its nash equilibrium execution.
- The details are shown in Appendix.  $\square$

#### Correctness of **SOSinLeave**()

The way to prove the correctness of **SOSinLeave**() is similar to that of **NESinLeave**(). We will give the outline of the proofs.

We can formalize **LocSoOp**( $D$ ) as a mapping  $\alpha' : \mathcal{V}(D) \rightarrow \mathbb{R}$ , so on  $k$ th iteration, we have  $\sigma'_k(G_i) = Ps_k(G_i)$ . **Refs**() defines a set of vertex  $\{G_i(\sigma'_k) \mid G_i(\sigma'_k) \text{ denotes } G_i \text{ with } e_{ij} \text{ whose sum of absolute weight pair is refreshed by the rule: } L_{k+1}^S(e_{ij}) = L_{WeIP}^S(e_{ij}) + \beta \cdot L_{TransP}(e_{ij}) \cdot \sigma'_k(G_j)\}$ . According to the rules of **SOSinLeave**( $D$ ), for any  $G_i \in \mathcal{V}(D)$ ,  $\sigma'_{k+1}(G_i) = Ps_1(G_i(\sigma'_k))$ . It is convenient to define another shorthand operator notation  $(T'\sigma')(G_i) = Ps_1(G_i(\sigma'))$ , that is  $T'\sigma'_k = \sigma'_{k+1}$ . By the same way as Lemma 3.1 and Lemma 3.2, we can prove operator  $T'$  is a contraction.

LEMMA 3.3. For any  $G_i \in \mathcal{V}(D)$ , we have

$$|\sigma'_k(G_i) - T'\sigma'_k(G_i)| \leq \max_{e \in E(G_i)} |L_k^S(e) - L_{k+1}^S(e)|$$

PROOF. The proof is similar to that of Lemma 3.1.  $\square$

LEMMA 3.4.  $T'$  is a contraction.

PROOF. The proof is similar to that of Lemma 3.2.  $\square$

THEOREM 3.4. If  $D$  is a Leave of **Abs**, then the result obtained by **SOSinLeave**( $D$ ) is SOS of  $D$ .

PROOF. The proof is similar to that of Theorem 3.3.  $\square$

#### Correctness of **AlgNES**() and **AlgSOS**()

THEOREM 3.5. The results obtained from **AlgNES**(**Abs**) and **AlgSOS**(**Abs**) are NES and SOS of **Abs** respectively.

PROOF. We prove the correctness of **AlgNES**(**Abs**) in details. Prove inductively on priority of vertex  $D$  in **Abs**.

- (1) If  $D$  is a Leave, we need to prove the result of **NESinLeave**( $D$ ) is NES of  $D$ , according to Theorem 3.3, trivial;
- (2) For Non-Leave  $D$ , and we assume  $prior(D) = prior(D') - 1$ , by induction hypothesis,  $D'$  has got its NES by **AlgNES**(). If  $\mathcal{V}(D) = \{G_i\}$  for some  $G_i \in V$ , according to the definition of **NEE** and rules of **BackInd**(), the proof is trivial; if the size of  $\mathcal{V}(D)$  is bigger than 1, according to the theorem 3.3, trivial.  $\square$

## 4. CASE STUDY

The details of the example we used can be found in [12]. It shows a local network connected to Internet (see Figure 3). By the assumption that the firewall is unreliable, and the operating system on the machine is insufficiently hardened, the attacker has chance to pretend as a root user in web server and steal or damage data stored in private file server and private workstation. The state set  $S$  of example is shown in

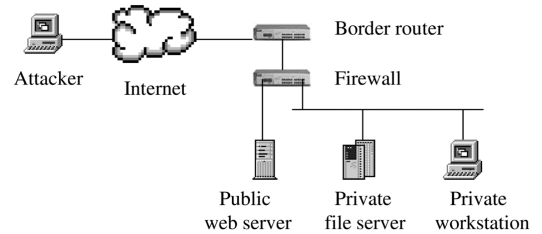


Figure 3: Case study

Table 3;  $A^a$ ,  $A^d$  is given in Table 5 and Table 4 respectively; for convenience, we will mostly refer to the states and actions using their symbolic number; state transition probability is shown in Table 7, in which  $\dot{p}(s_1, 1, 2, s_1) = P(1|1, 1, 2)$ ; the immediate payoff to attacker and defender at each state is shown in Table 6, in which  $\dot{r}^a(s_1, 2, \cdot) = R^1(1, 2, \cdot)$  and  $\dot{r}^d(s_1, 2, \cdot) = R^2(1, 2, \cdot)$ , where  $\cdot$  means any action available at current state.

### 4.1 Modeling for Case study



We modeling for state  $s_1$  in **ComModel** as example, then we have  $pA_1$ ,  $pD_1$ ,  $pN_1$  as follows:

$$\begin{aligned}
pA_1 &\stackrel{def}{=} \sum_{u \in A^a(s_1)} \overline{Attc}(u). \overline{Tell_d}(y). Nil \\
pD_1 &\stackrel{def}{=} \overline{Tell_a}(x). \sum_{v \in A^d(s_1)} \overline{Defd}(v). Nil \\
pN_1 &\stackrel{def}{=} \overline{Attc}(x). \overline{Tell_a}. \overline{Defd}(y). \overline{Tell_a}. Tr_1(x, y) \\
Tr_1(x, y) &\stackrel{def}{=} \sum_{\substack{u \in A^a(s_1) \\ v \in A^d(s_1)}} \overline{Log}(u, v). (if (x = u, y = v) then \\
&\quad \sum_{j \in I} [\dot{p}(s_i, u, v, s_j)] \overline{Rec}(\dot{r}(s_i, u, v)). (pA_j | pD_j | pN_j) \\
&\quad else Nil)
\end{aligned}$$

We find three pairs of states which are probabilistic bisimilar:  $s_{13} \sim s_{15}$ ,  $s_{14} \sim s_{16}$  and  $s_{17} \sim s_{18}$ . Figure 4 shows the **ConTS** of case study.

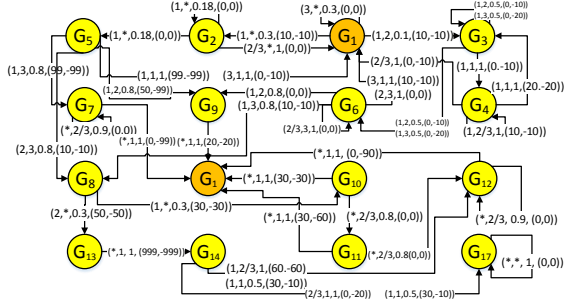


Figure 4: ConTS of Example

## 4.2 Analyzing NES/SOS for Case study

We implement the algorithms using Java in Eclipse development environment on machine with 3.4GHz Inter(R) Core(TM) i72.99G RAM. We get two Nash Equilibrium Strategies and one Social Optimal strategy for our case study, shown in Figure 5, 6, 7 respectively.

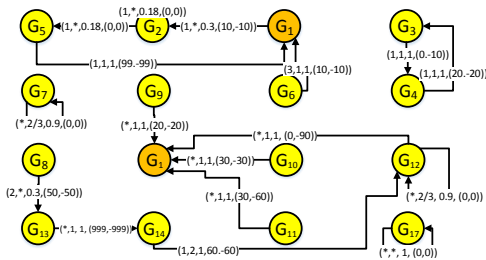


Figure 5: Nash Equilibrium strategy 1

## 4.3 Evaluation

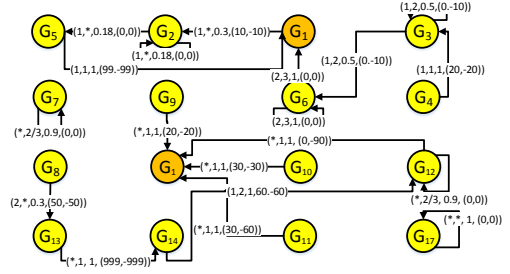


Figure 6: Nash Equilibrium strategy 2

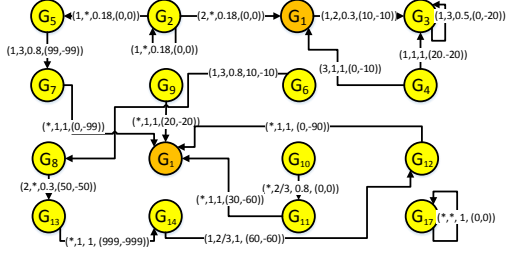


Figure 7: Social Optimal strategy

We compare our results with those obtained in [12] by game-theoretic approach:

- (1) We filter the invalid Nash Equilibrium strategy from the results in [12]. We filter the action pair  $(\phi, \text{Remove\_Sniffer\_Detector})$  at state  $s_3$  and the action pair  $(\text{Install\_Sniffer\_Detector}, \text{Remove\_Compromised\_account\_restart\_ftpd})$  at  $s_6$  which obtained in the second Nash Equilibrium strategy in [12] but have no practical state transition.
- (2) We minimize the state space by probabilistic bisimulation while [12] focuses on the whole state set. Time consumed to compute Nash Equilibrium strategy and Social Optimal strategy for this example with our approach is shown in Table 2. Although it is incomparable with the time consumed in [12] because of evaluating on different machine models, our approach should be faster theoretically.

ComModel Creation	Nash Equilibrium strategy	Social Optimal strategy
2.8s	3.7s	1.4s

Table 2: Time consumed for example with our approach

## 5. CONCLUSION

We proposed a probabilistic value-passing CCS (PVCCS) approach for modeling and analyzing a typical network security scenario with one attacker and one defender which is usually modeled by perfect and complete information game. Extension of this method might provide uniform framework for modelling and analyzing network security scenarios which are usually modeled via different games. We designed two algorithms for computing Nash Equilibrium strategy and Social Optimal strategy based on this PVCCS approach and on graph-theoretic methods. Advantages of these algorithms

are also discussed.

## 6. REFERENCES

- [1] M. Abadi and A. D. Gordon. A calculus for cryptographic protocols: The spi calculus. In *The 4th ACM Conf on Computer and Communications Security*, 1997.
- [2] J. Bergstra and J. Klop. Verification of an alternating bit protocol by means of process algebra. Technical report, Centrum voor Wiskunde en Informatica, 1984.
- [3] K. Chatzikokolakis, D. Gebler, C. Palamidessi, and L. Xu. Generalized bisimulation metrics. In *Proc. of CONCUR*, volume 8704, pages 32–46, 2014.
- [4] Y. Deng. *Semantics of probabilistic process—An operational approach*. Springer, 2014.
- [5] R. Diestel. *Graph Theory*. Springer-Verlag, 3 edition, 2005.
- [6] D. Easley and J. Kleinberg. *Networks, Crowds, and Markets: Reasoning about a Highly Connected World*. Cambridge University Press, 2010.
- [7] J. C. HARSANYI. Games with incomplete information played by bayesian players, i-iii. *Management Science*, 14(3), 1967.
- [8] E. M. Jean Tirole. Markov perfect equilibrium. *Journal of Economic Theory*, 2001.
- [9] J. Jormakka and J. Molsa. Modelling information warfare as a game. In *Journal of Information Warfare*, volume 4 of 2, 2005.
- [10] a. T. B. K. C. Nguyen, T. Alpcan. Stochastic games for security in networks with interdependent nodes. In *Proc. of Intl. Conf. on Game Theory for Networks (GameNets)*, 2009.
- [11] X. Liang and Y. Xiao. Game theory for network security. In *IEEE Communications Surveys and amp Tutorials*, 2013.
- [12] K. Lye and J. Wing. Game strategies in network security. In *Proceedings of the Foundations of Computer Security*, 2005.
- [13] R. Milner. *Communication and Cocurrency*. Prentice Hall International Ltd, 1989.
- [14] M. J. Osborne. *An Introduction to Game Theory*. Oxford University Press., 2000.
- [15] M. J. Osborne and A. Rubinstein. *A course in Game Theory*. MIT Press, 1994.
- [16] A. Patcha and J. Park. A game theoretic apporach to modeling intrusion detection in mobile ad hoc networks. In *Proceedings of the 2004 IEEE workshop on Information Assurance and Security*, 2004.
- [17] S. Roy and C. Ellis. A survey of game theory as applied to network security. In *43<sup>rd</sup> Hawaii International Conference on System Sciences*, 2010.
- [18] D. Sangiorgi. *An introduction to Bisimulation and Coinduction*. Springer, 2007.
- [19] I. M. Serge Abiteboul and P. Rigaux. *Web data management*. Cambridge University Press, 2011.
- [20] L. Shapley. *Stochastic Games*. Princeton University press, 1953.
- [21] P. Syverson. A different look at secure distributed computation. In *Proc. 10th IEEE Computer Security Foundations Workshop*, 1997.
- [22] R. van Glabbeek, S. A. Smolka, B. Steffen, and C. M. Tofts. Reactive, generative, and stratified models of probabilistic processes. In *Information and Computation*, 1995.
- [23] J. V. D. Wal. Stochastic dynamic programming. In *Mathematical Centre Tracts 139*. Morgan Kaufmann, 1981.
- [24] C. Xiaolin, T. Xiaobin, Z. Yong, and X. Hongsheng. A markov game theory-based risk assessment model for network information systems. In *International conference on computer science and software engineering*, 2008.

## APPENDIX

### A. PROOFS OF THEOREMS

Proof of Theorem 3.1

PROOF. As vertex set  $V$  is finite, then any infinite execution  $\pi_i$  of  $G_i$  is in form of  $G_i e_{i1} G_1 \dots (G_k \dots G_{(k+m)} e_{(k+m)k} G_k)$  which means ending with a cycle starting with  $G_k$ , and  $m$  is the number of vertex on this cycle except  $G_k$ , then we have

$$\begin{aligned} PF^a(\pi_i) &= L_{Weip}^a(e_{i1}) + \beta \cdot PF^a(\pi_i[1]) \\ &= L_{Weip}^a(e_{i1}) + \dots + \beta^k \cdot PF^a(\pi_i[k]) \\ &= A + \beta^k \cdot PF^a(\pi_i[k]) \end{aligned}$$

$$\begin{aligned} \text{where } A &= L_{Weip}^a(e_{i1}) + \dots + \beta^{k-1} \cdot L_{Weip}^a(e_{(k-1)k}) \\ PF^a(\pi_i[k]) &= L_{Weip}^a(e_{k(k+1)}) + \dots + \beta^m \cdot L_{Weip}^a(e_{(k+m)k}) \\ &\quad + \beta^{m+1} \cdot B + \beta^{2m+2} \cdot B + \dots \\ &= (B \cdot \frac{1 - \beta^{(m+1)h}}{1 - \beta^{(m+1)}})_{h \rightarrow \infty} \end{aligned}$$

$$\text{where } B = L_{Weip}^a(e_{k(k+1)}) + \dots + \beta^m \cdot L_{Weip}^a(e_{(k+m)k})$$

$$\begin{aligned} \lim_{h \rightarrow \infty} PF^a(\pi_i) &= \lim_{h \rightarrow \infty} (A + \beta^k (B \cdot \frac{1 - \beta^{(m+1)h}}{1 - \beta^{(m+1)}})) \\ &= A + \beta^k \cdot B \cdot \lim_{h \rightarrow \infty} (\frac{1 - \beta^{(m+1)h}}{1 - \beta^{(m+1)}}) \\ &= A + B \cdot \frac{\beta^k}{1 - \beta^{(m+1)}} \end{aligned}$$

□

Proof of Lemma 3.1

PROOF. Assuming without loss of generality,  $\sigma_k(G_i) = (L_k(e_1)^a, L_k(e_1)^d)$  and  $T\sigma_k(G_i) = (L_{k+1}(e_2)^a, L_{k+1}(e_2)^d)$ , where  $e_1, e_2 \in E(G_i)$ . Let  $L_k^a(e_1) = a, L_k^d(e_2) = b, L_{k+1}^a(e_1) = a'$  and  $L_{k+1}^d(e_2) = b'$ , where  $a, a', b, b'$  are positive number.

**case 1:**  $L_{Act}^a(e_1) = L_{Act}^a(e_2)$

According to the rules of **BackInd**(), we have  $a < b$  and  $b' < a'$ . If the first inequality in lemma doesn't hold, then we have  $|a - b'| > |a - a'|$  and  $|a - b'| > |b - b'|$ , then we get  $(b' - a')(b' + a') > 2a(b' - a')$  and  $(a - b)(a + b) > 2b'(a - b)$  which deduce  $a - b > a' - b'$ , contradiction.

**case 2:**  $L_{Act}^a(e_1) \neq L_{Act}^a(e_2)$

Let us define two conditions:

Cond 1: on  $k$ th iteration,  $e_2$  is kept by step (2) of **BackInd**() .

Cond 2: on  $(k+1)$ th iteration,  $e_1$  is kept by step (2) of **BackInd**() .

There are four subcases to be considered:

**case 2.1:** both Cond 1 and Cond 2

According to the rules of **BackInd**(), we have  $a > b$  and  $b' > a'$ . If  $|a - b'| > |a - a'|$  and  $|a - b'| > |b - b'|$ , then we get  $b - a > b' - a'$ , contradiction.

**case 2.2:** not Cond 2 but Cond 1

According to the rules of **BackInd**(),  $\exists e'$  with  $L_{Act}^a(e') = L_{Act}^a(e_1)$ . Assuming  $L_k^a(e') = c$  and  $L_{k+1}^a(e') = c'$ , then we have  $c > a > b, a' > c'$  and  $b' > c'$ . If  $|a - b'| > |a - a'|$  and  $|a - b'| > |b - b'|$ , then we have  $(b' - a')(b' + a') > 2a(b' - a')$  and  $a + b > 2b'$ . If  $b' > a' > c'$ , it is trivial to get contradiction; If  $c' < b' < a'$ , then we have  $2b' < b' + a' < 2a$  and  $2c > a + b > 2b' > 2c'$ , then we have  $b' < a$  and  $c > c'$ . If  $|a - b'| > |c - c'|$ , then we have  $a - c > b' - c'$ , contradiction;

If  $b' = a'$ , contradiction.

**case 2.3:** not Cond 1 but Cond 2

According to the rules of **BackInd**(),  $\exists e'$  with  $L_{Act}^a(e') = L_{Act}^a(e_2)$ . proof is similar to **case 2.2**.

**case 2.4:** neither Cond 1 nor Cond 2

According to the rules of **BackInd**(),  $\exists e', e''$  with  $L_{Act}^a(e') = L_{Act}^a(e_1)$  and  $L_{Act}^a(e'') = L_{Act}^a(e_2)$ . Assuming  $L_k^a(e') = c$  and  $L_{k+1}^a(e') = c', L_k^a(e'') = d$  and  $L_{k+1}^a(e'') = d'$ , then we have  $d < a < c, d < b, a' > c'$  and  $c' < b' < d'$ . If  $|a - b'| > |a - a'|$  and  $|a - b'| > |b - b'|$ , then we have  $(b' - a')(b' + a') > 2a(b' - a')$  and  $(a - b)(a + b) > 2b'(a - b)$ . If  $a > b$  and  $a' > b'$ , then we have  $c' < c$  and  $a > b'$ , and if  $|a - b'| > |c - c'|$ , then we have  $a - c > b' - c'$ , contradiction; If  $a < b$  and  $a' > b'$  or  $a > b$  and  $a' < b'$ , it is trivial to get contradiction; If  $a < b$  and  $a' < b'$ , then we get  $d' > d$  and  $a < b'$ , and if  $|a - b'| > |d - d'|$ , then we get  $b' - d' > a - d$ , contradiction.

Proof for second inequality is similar. We skip the details.

□

Proof for Theorem 3.3.

PROOF. We need to prove two issues:

1. **NESinLeave**( $D$ ) is terminated.

The way to prove termination of **NESinLeave**( $D$ ) is to prove  $\exists k$  that after  $k$ th iteration,  $\forall G_i, Pp_k(G_i) = Pp_{k+1}(G_i)$ . According to Lemma 3.2, trivial;

2. The result of **NESinLeave**( $D$ ) is *NES* of  $D$ .  $\forall G_i \in \mathcal{V}(D)$ , assuming  $\pi_i$  whose first edge is  $e$  is the execution of  $G_i$  based on the result obtained by **NESinLeave**( $D$ ), we need to prove  $\pi_i^e$  is *NEE* of  $G_i$  coinductively. As  $\pi_i^e$  is ended by a cycle, we just need to prove any  $e'$  on  $\pi_i^e, e' \in E(G_j)$ , is the first edge of *NEE* of  $G_j$ . We prove edge  $e$  of  $G_i$  as example. If  $\pi_i^e$  is not *NEE* of  $G_i$ , according to the definition of *NEE*, there exists  $\pi_i^{e'}$  satisfying: (1)  $PF^d(\pi_i^{e'}) > PF^d(\pi_i^e)$  where  $L_{Act}^a(e') = L_{Act}^a(e)$  or (2)  $PF^a(\pi_i^{e'}) > PF^a(\pi_i^e)$  where  $e' = \arg \max_{e'' \in E^a(G_i, e')} PF^d(\pi_i^{e''})$ , and both of them are contradicted with the rules in **BackInd**() .

□

### B. TABLES OF CASE STUDY

To make paper self-contained, we list the data related in example created in [12].

State number	State name
1	Normal_operation
2	Httpd_attacked
3	Ftp_attacked
4	Ftpd_attacked_detector
5	Httpd_hacked
6	Ftpd_hacked
7	Website_defaced
8	Webserver_sniffer
9	Webserver_sniffer_detector
10	Webserver_DOS_1
11	Webserver_DOS_2
12	Network_shutdown
13	Fileserver_hacked
14	Fileserver_data_stolen
15	Workstation_hacked
16	Workstation_data_stolen_1
17	Fileserver_data_stolen
18	Workstation_data_stolen_2

Table 3: Network state

State no.\ Action no.	1	2	3
1	$\phi$	$\phi$	$\phi$
2	$\phi$	$\phi$	$\phi$
3	Install_Sniffer_ Detector	$\phi$	$\phi$
4	Remove_Sniffer_ Detector	$\phi$	$\phi$
5	Remove_Compromised_ account_restart_httpd	Install_sniffer_ detector	$\phi$
6	Remove_Compromised_ account_restart_ftpd	Install_sniffer_ detector	$\phi$
7	Restore_website_remove_ compromised_account	$\phi$	$\phi$
8	$\phi$	$\phi$	$\phi$
9	Remove_sniffer_and_ Compromised_account	$\phi$	$\phi$
10	Remove_virus_and_ Compromised_account	$\phi$	$\phi$
11	Remove_virus_and_ Compromised_account	$\phi$	$\phi$
12	Remove_virus_and_ Compromised_account	$\phi$	$\phi$
13	$\phi$	$\phi$	$\phi$
14	Remove_sniffer_and_ Compromised_account	$\phi$	$\phi$
15	$\phi$	$\phi$	$\phi$
16	Remove_sniffer_and_ Compromised_account	$\phi$	$\phi$
17	$\phi$	$\phi$	$\phi$
18	$\phi$	$\phi$	$\phi$

Table 4: Defender's action set

State no.\ Action no.	1	2	3
1	Attack_httpd	Attack_ftpd	$\phi$
2	Continue_ attacking	$\phi$	$\phi$
3	Continue_ attacking	$\phi$	$\phi$
4	Continue_ attacking	$\phi$	$\phi$
5	Deface_ website	Install_ sniffer	$\phi$
6	Install_ sniffer	$\phi$	$\phi$
7	$\phi$	$\phi$	$\phi$
8	Run_DOS_ virus	Crack_fileservers_ root_password	Crack_workstation_ root_password
9	$\phi$	$\phi$	$\phi$
10	$\phi$	$\phi$	$\phi$
11	$\phi$	$\phi$	$\phi$
12	$\phi$	$\phi$	$\phi$
13	Capture_ data	$\phi$	$\phi$
14	Shutdown_ network	$\phi$	$\phi$
15	Capture_ data	$\phi$	$\phi$
16	Shutdown_ network	$\phi$	$\phi$
17	$\phi$	$\phi$	$\phi$
18	$\phi$	$\phi$	$\phi$

Table 5: Attacker's action set

$R^1(1) = \begin{bmatrix} 10 & 10 & 10 \\ 10 & 10 & 10 \\ 0 & 0 & 0 \end{bmatrix}$	$R^2(1) = -R^1(1)$
$R^1(2) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$	$R^2(2) = R^1(2)$
$R^1(3) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$	$R^2(3) = \begin{bmatrix} -10 & -10 & -20 \\ -10 & -10 & 0 \\ -10 & -10 & 0 \end{bmatrix}$
$R^1(4) = \begin{bmatrix} 20 & 10 & 10 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$	$R^2(4) = \begin{bmatrix} -20 & -10 & -10 \\ -10 & 0 & 0 \\ -10 & 0 & 0 \end{bmatrix}$
$R^1(5) = \begin{bmatrix} 99 & 50 & 99 \\ 10 & 0 & 10 \\ 0 & 10 & 0 \end{bmatrix}$	$R^2(5) = \begin{bmatrix} -99 & -99 & -99 \\ 10 & 10 & -10 \\ -10 & -10 & 0 \end{bmatrix}$
$R^1(6) = \begin{bmatrix} 0 & 0 & 10 \\ 10 & 0 & 0 \\ 10 & 0 & 0 \end{bmatrix}$	$R^2(6) = -R^1(6)$
$R^1(7) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$	$R^2(7) = \begin{bmatrix} -99 & 0 & 0 \\ -99 & 0 & 0 \\ -99 & 0 & 0 \end{bmatrix}$
$R^1(8) = \begin{bmatrix} 30 & 30 & 30 \\ 50 & 50 & 50 \\ 50 & 50 & 50 \end{bmatrix}$	$R^2(8) = -R^1(8)$
$R^1(9) = \begin{bmatrix} -20 & 0 & 0 \\ -20 & 0 & 0 \\ -20 & 0 & 0 \end{bmatrix}$	$R^2(9) = R^1(9)$
$R^1(10) = \begin{bmatrix} 30 & 0 & 0 \\ 30 & 0 & 0 \\ 30 & 0 & 0 \end{bmatrix}$	$R^2(10) = -R^1(10)$
$R^1(11) = \begin{bmatrix} 30 & 0 & 0 \\ 30 & 0 & 0 \\ 30 & 0 & 0 \end{bmatrix}$	$R^2(11) = \begin{bmatrix} -60 & 0 & 0 \\ -60 & 0 & 0 \\ -60 & 0 & 0 \end{bmatrix}$
$R^1(12) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$	$R^2(12) = \begin{bmatrix} -90 & 0 & 0 \\ -90 & 0 & 0 \\ -90 & 0 & 0 \end{bmatrix}$
$R^1(13) = \begin{bmatrix} 999 & 0 & 0 \\ 999 & 0 & 0 \\ 999 & 0 & 0 \end{bmatrix}$	$R^2(13) = -R^1(13)$
$R^1(14) = \begin{bmatrix} 30 & 60 & 60 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$	$R^2(14) = \begin{bmatrix} -10 & -60 & -60 \\ -20 & 0 & 0 \\ -20 & 0 & 0 \end{bmatrix}$
$R^1(15) = \begin{bmatrix} 999 & 0 & 0 \\ 999 & 0 & 0 \\ 999 & 0 & 0 \end{bmatrix}$	$R^2(15) = -R^1(13)$
$R^1(16) = \begin{bmatrix} 30 & 60 & 60 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$	$R^2(16) = \begin{bmatrix} -10 & -60 & -60 \\ -20 & 0 & 0 \\ -20 & 0 & 0 \end{bmatrix}$
$R^1(17) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$	$R^2(17) = R^1(17)$
$R^1(18) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$	$R^2(18) = R^1(18)$

Table 6: Immediate payoff to Attacker and Defender

<b>State 1</b> $p(2 1, 1, \cdot) = 1/3$ $p(3 1, 1, 2) = 1/3$ $p(1 1, 3, \cdot) = 1/3$	<b>State 2</b> $p(2 2, 1, \cdot) = 0.5/3$ $p(5 2, 1, \cdot) = 0.5/3$ $p(1 2, 2, \cdot) = 1$ $p(1 2, 3, \cdot) = 1$	<b>State 3</b> $p(3 3, 1, 2) = 0.5$ $p(3 3, 1, 3) = 0.5$ $p(6 3, 1, 2) = 0.5$ $p(6 3, 1, 3) = 0.5$ $p(4 3, 1, 1) = 1$
<b>State 4</b> $p(1 4, 2, 1) = 1$ $p(1 4, 3, 1) = 1$ $p(3 4, 1, 1) = 1$ $p(4 4, 1, 2) = 1$ $p(4 4, 1, 3) = 1$	<b>State 5</b> $p(7 5, 1, 3) = 0.8$ $p(8 5, 2, 3) = 0.8$ $p(9 5, 1, 2) = 0.8$ $p(1 5, 3, 1) = 1$ $p(1 5, 1, 1) = 1$	<b>State 6</b> $p(8 6, 1, 3) = 0.8$ $p(9 6, 1, 2) = 0.8$ $p(1 6, 2, 3) = 1$ $p(1 6, 3, 1) = 1$ $p(6 6, 2, 3) = 1$ $p(6 6, 3, 3) = 1$
<b>State 7</b> $p(1 7, \cdot, 1) = 1$ $p(7 7, \cdot, 2) = 0.9$ $p(7 7, \cdot, 3) = 0.9$	<b>State 8</b> $p(10 8, 1, \cdot) = 1/3$ $p(13 8, 2, \cdot) = 0.3$ $p(15 8, 3, \cdot) = 0.3$	<b>State 9</b> $p(1 9, \cdot, 1) = 1$
<b>State 10</b> $p(1 10, \cdot, 1) = 1$ $p(11 10, \cdot, 2) = 0.8$ $p(11 10, \cdot, 3) = 0.8$	<b>State 11</b> $p(1 11, \cdot, 1) = 1$ $p(12 11, \cdot, 2) = 0.8$ $p(12 11, \cdot, 3) = 0.8$	<b>State 12</b> $p(1 12, 1, \cdot) = 1$ $p(12 12, \cdot, 2) = 0.9$ $p(12 12, \cdot, 3) = 0.9$
<b>State 13</b> $p(14 13, 1, \cdot) = 1$	<b>State 14</b> $p(12 14, 1, 2) = 1$ $p(12 14, 1, 3) = 1$ $p(17 14, 2, 1) = 1$ $p(17 14, 3, 1) = 1$ $p(12 14, 1, 1) = 0.5$ $p(17 14, 1, 1) = 0.5$	<b>State 15</b> $p(16 15, 1, \cdot) = 1$
<b>State 16</b> $p(12 16, 1, 2) = 1$ $p(12 16, 1, 3) = 1$ $p(18 16, 2, 1) = 1$ $p(18 16, 3, 1) = 1$ $p(12 16, 1, 1) = 0.5$ $p(18 16, 1, 1) = 0.5$	<b>State 17</b> $p(17 17, \cdot, \cdot) = 0.9$	<b>State 18</b> $p(18 18, \cdot, \cdot) = 0.9$

**Table 7: State transition probabilities**

## C. NOTATION INDEX

<i>Abs</i> , 5	NESinNonLeave(), 7
AlgNES(), 5	$PF^a(\pi_i)$ , 4
AlgSOS(), 5	$PF^d(\pi_i)$ , 4
BackInd(), 6	$Pp_n(G_i)$ , 6
<b>ComModel</b> , 3	$Ps_n(G_i)$ , 6
ConTS, 4	PrePro(), 7
<i>D</i> , 5	PreProS(), 7
<i>execution</i> , 4	PVCCS <sub>R</sub> , 2
$L_n(e)$ , 6	RefN(), 6
$L_n^S(e)$ , 6	RefS(), 6
<i>Leave</i> , 5	<i>SOE</i> , 5
LocSoOp(), 6	<i>SOS</i> , 5
<i>NEE</i> , 5	SOSinLeave(), 6
<i>NES</i> , 5	SOSinNonLeave(), 7
NESinLeave(), 6	$\mathcal{V}(D)$ , 5